



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,108	07/15/2003	Marcus Janke	S&ZIO020101	8615
27346 7590 11/15/2007 LERNER GREENBERG STEMER LLP FOR INFINEON TECHNOLOGIES AG P.O. BOX 2480 HOLLYWOOD, FL 33022-2480			EXAMINER DAVIS, ZACHARY A	
			ART UNIT 2137	PAPER NUMBER
			MAIL DATE 11/15/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

**Application No.**

10/620,108

**Applicant(s)**

JANKE, MARCUS

**Examiner**

Zachary A. Davis

**Art Unit**

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 31 August 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. A response to the notice of non-compliant amendment was received on 31 August 2007. By this response, Claims 1, 2, and 4-16 have been amended. New Claim 17 has been added. No claims have been canceled. Claims 1-17 are currently pending in the present application.

### ***Response to Arguments***

2. Applicant's arguments with respect to claims 1-17 have been considered but are moot in view of the new ground(s) of rejection.

### ***Specification***

3. The objection to the disclosure is not withdrawn. Although Applicant has corrected many of the errors noted in the previous Office action, other errors remain, and the amendments have also introduced new issues.

4. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, although Applicant has replaced the term "energy" with "power" throughout the specification, the phrase "supply power" is still not a common usage; it appears that "power supplied", "supplied power", or simply "power" would be more appropriate.

Art Unit: 2137

Further, in the amendments at pages 4, 5, 6, and 8 of the present response, it appears that the word "aspect" should have been retained in the phrases "In accordance with a first [second, third, fifth] aspect" instead of being replaced by "object". In the amendment on page 9 of the present response, the phrase "The remainder of the algorithm code not having been received" is still generally awkwardly worded. In the amendment on page 12 of the present response, the phrase "whereby it is further aggravated for a potential attacker to find out the algorithm code employed" is still generally narrative and unclear, in particular with regard to the use of the term "aggravated". In the amendment at line 2 of page 15 of the present response, as previously noted, it appears that "chard" is intended to read "card". In the amendment on page 16 of the present response, the phrase "the chip card 10 longer operates for a predetermined period of time" is still generally unclear, particularly in the phrasing "longer operates". In the amendment on page 18 of the present response, it appears that "loosing" is intended to read "losing"; further, in the parenthetical phrase "whereby - if successful, these would come into possession of the complete algorithm code", it is not clear what the antecedent of the term "these" is intended to be.

Appropriate correction is required. Again, the Examiner notes that the above is not considered to be an exhaustive list of errors and that the lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is again requested in correcting any other errors of which applicant may become aware in the specification.

***Claim Objections***

5. The objections to Claims 1, 11, and 13-15 are not withdrawn; although Applicant has corrected informalities noted in the previous Office action, the amendments have introduced new issues.

6. Claims 1, 11, 13-15, and 17 are objected to because of the following informalities:

Claims 1, 11, 13-15, and 17 each include the limitation "supply power". This is still uncommon usage; it appears that this should be replaced by "supplied power", "power supplied", or simply "power".

In Claim 14, it appears that a comma should be inserted after "controlling" at the end of line 1.

Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

7. The rejection of Claims 1-5, 8, and 10 under 35 U.S.C. 112, second paragraph, is withdrawn in light of the amendments to the claims, and in light of the description of where in the present specification the term "jump address" is defined (see page 36 of the present response). The remaining claims remain rejected because the issues have not been addressed and/or the amendments to the claims have raised further issues of indefiniteness.

Art Unit: 2137

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 6, 7, 9, and 11-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 6 recites the limitation "selected from a plurality of conditions comprising..." This is not a proper Markush claim, because it uses "comprising" instead of "consisting of". Therefore, it does not clearly set forth all of the possible alternatives encompassed by the claims. It is uncertain what the scope of the claims is. See MPEP § 2173.05(h) I. Further, the phrase "as well as of additional operating parameters" renders the claim indefinite because the claim includes elements not actually disclosed (those encompassed by "additional parameters"), thereby rendering the scope of the claim unascertainable. See MPEP § 2173.05(d). Additionally, it is not clear what exactly is encompassed by the terms "irregularity" and "fluctuation".

Claim 7 recites the limitation "as well as an access function for changing". This is unclear because the use of "as well as" makes it unclear whether the access function for changing is a part of the group from which the task is selected. It is further noted that a Markush group is typically referred as "the group consisting of..." rather than "a group consisting of..." as in the claim.

Claim 9 recites the limitation "storing a newly received version of one of the part of the algorithm code and the complete algorithm code such that the previously received version of one of the part of the algorithm code and the complete algorithm code is

Art Unit: 2137

overwritten” is still somewhat narrative and unclear; further, there is insufficient antecedent basis for the phrase “the previously received version”.

Claim 11 recites the limitation “the supply power” at lines 14-15 of the claim.

There is insufficient antecedent basis for this limitation in the claim.

Claim 13 recites the limitation “with the terminal, for each communication operation between terminal and security module, being adapted to, during a single one of the communication operations with the security module, send at least the part of the algorithm code or the complete algorithm code to the volatile memory of the security module”. This is still generally unclear; it appears that the phrases “for each communication operation...” and “during a single one of the communication operations” contradict each other. Further, the limitation “after sending, receive the algorithm code result from the security module” is generally unclear, as it is not clear what the subject of this limitation is, nor is it clear how this is a structural limitation limiting the claimed terminal.

Claim 14 recites the limitation “A process for controlling within a plurality of communication operations, a security module using a terminal”; this appears to read that the security module is within the plurality of communication operations, but that would not appear to be a plausible situation. Further, the claim recites the limitation “for each communication operation, performing the following steps during a single one of the communication operations”; it appears that the phrases “for each communication operation” and “during a single one of the communication operations” contradict each other.

Claim 15 recites the limitation "with the volatile memory being supplied by supply power" in lines 10-11 of the claim. This is generally unclear, as it is not clear from whence the power is supplied.

Claim 17 recites the limitation "a non-volatile memory in which a second part of the algorithm code which is a non-received remainder the algorithm code is stored". This is generally unclear and narrative. First, the phrase "non-received" is generally unclear in itself; second, if the remainder is "non-received" then it is not clear how it is possible to store it; and third, the phrase "a non-received remainder the algorithm code is stored" appears to be missing language.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

### ***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takahira, US Patent 4777355 (see the information disclosure statement received 15 December 2003), in view of Schneier et al, US Patent 5768382.

In reference to Claim 1, Takahira discloses a security module (Figure 1, IC card 1) including a data interface that receives algorithm code (see Figure 1; column 3, lines 24-38; column 4, lines 4-33); an interface for receiving power (see Figure 1; column 3, lines 24-38); a memory storing the algorithm code, where the memory can be cleared (Figure 1, programmable memories 4 and 4A; column 4, lines 4-33; column 6, lines 13-20); and a processor that performs the algorithm code to determine a result (Figure 1, microprocessor 2; column 3, lines 32-35; column 5, lines 9-35). However, Takahira does not explicitly disclose that the algorithm code is for processing secrets, nor does Takahira explicitly disclose clearing the memory when the power supply is interrupted.

Schneier discloses a security module (column 11, lines 34-44; column 7, lines 38-41; column 12, lines 6-44) including a data interface that includes algorithm code concerning a processing of secrets (column 14, lines 19-21); an interface for receiving power (Figure 4D, power 27); a volatile memory storing the received algorithm code, where the volatile memory is cleared when the power supply is interrupted (Figure 4D, volatile memory 23b; column 14, lines 22-26); and a processor for performing the algorithm code (Figure 4C, CPU 302; column 11, lines 55-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the module of Takahira to include the features of Schneier, in order to increase security as desired by Takahira (Takahira, column 6, lines 16-20; column 4, lines 62-65) by making hardware tamper-resistant in order to protect data and algorithms that must remain secure (see Schneier, column 11, lines 34-37).

In reference to Claim 2, Takahira and Schneier further disclose non-volatile memory storing a remainder of algorithm code (Takahira, Figure 1, ROM 3, and column 3, lines 39-58; Schneier, column 14, lines 17-19).

In reference to Claim 3, Takahira and Schneier further disclose means for performing authentication (Schneier, column 20, lines 15-26).

In reference to Claim 4, Takahira and Schneier further disclose receiving a certificate and examining a certificate, and decrypting code (Schneier, column 14, lines 17-26; column 44, lines 30-35; column 50, lines 36-37).

In reference to Claims 5 and 8, Takahira and Schneier further disclose a memory managing unit and code that includes addresses (Takahira, column 3, lines 59-68; Schneier, column 7, lines 48-61).

In reference to Claim 6, Takahira and Schneier further disclose means for monitoring a predetermined security condition and clearing the volatile memory if the condition is fulfilled (Schneier, column 14, lines 19-26).

In reference to Claim 7, Takahira and Schneier further disclose that the algorithm code can perform a symmetric cryptographic algorithm such as DES or an asymmetric cryptographic algorithm such as RSA (see Schneier, column 9, line 58-column 10, line 11, and column 10, lines 27-40).

In reference to Claim 9, Takahira and Schneier further disclose updating the code (Takahira, column 5, lines 9-19; Schneier, column 14, lines 27-34).

In reference to Claim 10, Takahira and Schneier further disclose a chip card (Takahira, Figure 1, IC card 1; column 3, lines 12-38; Schneier, column 11, lines 34-44; column 7, lines 38-41; column 12, lines 6-44).

Claims 11 and 12 are directed to a method corresponding substantially to the module of Claim 1, and are rejected by a similar rationale.

In reference to Claim 13, Takahira discloses a terminal including a data interface that transmits algorithm code to a memory in a security module (see Figure 1; column 3, lines 24-38; column 4, lines 4-33) and an interface for supplying power (see Figure 1; column 3, lines 24-38). However, Takahira does not explicitly disclose that the algorithm code is for processing secrets, nor does Takahira explicitly disclose clearing the memory when the power supply is interrupted.

Schneier discloses a terminal including a data interface that transmits, to a volatile memory in a security module, algorithm code concerning a processing of secrets (column 14, lines 19-21; Figure 4D, volatile memory 23b) and an interface for supplying power such that the volatile memory is cleared if there is an interruption in the power supply (Figure 4D, power 27; column 14, lines 22-26). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the terminal of Takahira to include the features of Schneier, in order to increase security as desired by Takahira (Takahira, column 6, lines 16-20; column 4, lines 62-65).

Art Unit: 2137

by making hardware tamper-resistant in order to protect data and algorithms that must remain secure (see Schneier, column 11, lines 34-37).

Claim 14 is directed to a method corresponding substantially to the terminal of Claim 13, and is rejected by a similar rationale.

Claim 15 is directed to a method encompassing the performance of the methods of Claims 11 and 14 simultaneously, and is rejected by a similar rationale. Claim 16 recites limitations corresponding to those recited in Claim 9, and is rejected by a similar rationale.

Claim 17 is directed to a security module encompassing the limitations of Claims 1 and 8, and is rejected by a similar rationale.

### ***Conclusion***

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Weiss, US Patent 4720860, discloses a method for authentication that includes an algorithm stored on an IC card in volatile memory.

Art Unit: 2137

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD  
zad

  
G. J. Jones  
SUPERVISORY INVENTOR